REMARKS:

This paper is herewith filed in response to the Examiner's Office Action mailed on March 5, 2009 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-10 and 12-16 of the application.

More specifically, the Examiner has rejected claims "1-14" under 35 USC 103(a) as being unpatentable over Win (US6,453,353) in view of Wright (US20040123153). The Applicant respectfully traverses the rejections.

Claims 1, 4-5, 7, 9, 14, and16 have been amended for clarification. Support for the amendments can be found at least in Figure 3 and paragraphs [0044]-[0045], [0047]-[0048], and [0055]-[0057] of the published application. No new matter is added.

In the Response to Arguments section of the Office Action the Examiner states:

> "Applicant argues that the Win does not teach an automated security scan of the second network device to determine at least one of a hardware or software capability of the network device," and
>
> "In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *in re Keller,* 642 F.2d 413, 208 USPQ 871 (COPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)," and
>
> "Moreover, the examiner submits that Win does teach the feature of performing an automated security scan of a second network device by a first network device to determine a capability of the second network device as shown in line 8, col. 8, line 23-col. 9, line 40, col. 10, line 64-col. 12," and
>
> "Applicant argues that Wright does not teach or suggest the feature of performing an automated security scan of the second network device to determine at least one of a hardware or software capability of the network device. in response to applicant's argument, the examiner submits that Wright does teach performing an automated security scan of the second network device to determine at least one of

> a hardware or software capability of the network device as shown in paragraphs [0013-001 4], [00078]."

The Applicants respectfully disagree with the Examiner.

Firstly, with regards to the Examiner's comments that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references," the Applicants respectfully note that in the prior Response dated December 4, 2008 it was explicitly stated that "the Applicant submits that Wright, the additional reference cited against claim 1, can not be seen to address the above shortfalls of Win." Thus, the Applicants submit that, at least here, the deficiency of the proposed combination is seen to have been argued.

Further, the Applicants note that claim 1 has been amended to recite:

> A method, comprising: performing an automated security scan of a second network device by a first network device to determine at least one of a hardware or software capability of the second network device; determining an attribute for the second network device based, in part, on the determined capability; generating an attribute certificate for the second network device based in part on the attribute; storing the attribute certificate including the attribute on a device other than the second network device; receiving, at the first network device, an authentication request from the second network device for access to a resource over a network; verifying the authentication request from the second network device, or else terminating communication with the second network device; responsive to a verified authentication request from the second network device for access to a resource over a network, the first network device requesting and receiving from the other device the stored attribute certificate for the second network device; and the first network device determining whether the received attribute certificate for the second network device is valid, where if the attribute certificate is determined valid, authorizing access to the resource over the network based, in part, on the attribute associated with the attribute certificate, or else terminating communication with the second network device.

Support for the amendments can be found at least in Figure 3 and paragraphs [0044], [0047]-[0048], and [0055]-[0057] of the published application. The Applicants submit that claim 1, as amended, is patentably distinguishable from the references cited.

The Applicants note that for clarification of the arguments presented the Applicants have listed the following items pertaining to exemplary embodiments of the invention that are recited in claim 1. These items are as follows:

item 1 – **performing, by a first network device, an automated security scan** of a second network device in order to **determine its capabilities, determining** an attribute for the second network device **based in part on the determined capabilities, generating an attribute certificate** for the second network device **based in part on the attribute**, and storing the attribute certificate on a device other than the second network device,
item 2 – **receiving, at the first network device, an authentication request from the second network device** for access to a resource on a network, **then verifying the authentication request, or else terminating communication with the second network device,**
item 3 – **responsive to a verified authentication request, the first network device requesting and receiving the attribute certificate from a device other then the second network device,** and **the first network device determining the validity of the received attribute, or else terminating communication with the second network device**.

Reference item 1:

The Applicants submit that the references cited can not be seen to disclose or suggest at least where claim 1 recites in part:

> "performing an automated security scan of a second network device by a first network device to determine at least one of a hardware or software capability of the second network device; determining an attribute for the second network device based, in part, on the determined capability; generating an attribute certificate for the second network device based in part on the attribute; storing the attribute certificate including the attribute on a device other than the second network device"

First, with regards to Win it is noted that the Examiner states that "Win teaches a method,

comprising: performing an automated security scan of a second network device by a first network device to determine a capability of the second network device (line 8, col. 8, line 23-col. 9, line 40, col. 10, line 64-col. 12) [and] generating an attribute certificate the second network device based in part on the attribute (col. 7, line 34-col. 8, line 46, col. 10, line 34-col. 11, line 9)." The Applicants note that here the Examiner cites Win broadly without any specificity as to which language in Win is allegedly seen to disclose or suggest these features related to claim 1.

The Applicants submit that as cited Win discloses in a somewhat relevant part:

> "FIG. 3B is a state diagram showing processes carried out when the URL is a protected resource. As shown by state 312, Runtime Module 206 calls the Authentication Verification Service to check whether an authenticated user is making the request. An authenticated user is one who has successfully logged into the system. A user is considered authenticated if the request contains a "user cookie" that can be decrypted, and the request's IP address matches that in the cookie. If the conditions are not satisfied, then the user cannot be authenticated, and as shown in state 314, Runtime Module 206 returns a redirection to the Login URL. As shown by state 316, HTTP Server 202 returns the redirection to the Login URL to the browser 100," (emphasis added), (col.8, lines 23-35).

The Applicants note that in order to support where the rejection of claim 1 relates to performing an automated scan to determine a capability of the device, the Examiner appears to rely on where Win discloses that a user authentication request contain a "user cookie" that can be decrypted and that the "request's IP address" matches the IP address of the cookie.

The Applicants submit that although Win may relate to determining whether a cookie in a user's request can be decrypted and that an IP address of the cookie matches the "request's IP address," the Applicants submit that, as indicated above, these operations are performed by the runtime module 206 which is on the protected server in Win. Thus, the cookie which is said to be contained in the request is sent to the protected server. Further, the Applicants submit that any determinations of whether the cookie can be decrypted and whether the IP addresses match is made by the runtime module 206 on the protected server (see Fig. 2 and col. 23, lines 3-4).

In addition, the Applicants submit that to determine the IP address of the user making the request, the runtime module 206 need merely examine the source IP address of the packet data containing the request. The Applicants submit that there can not be found anything in all of Win which can be seen to disclose that the user device is scanned to determine its IP address. Therefore, the Applicants submit that these operations can not be seen to disclose or suggest performing an automated scan of the device to determine a capability of the device.

In addition, the Applicants note that the cookie included with the request can not be seen to be determined or generated using an automated scan of the user device. As will be discussed in more detail below, the cookie contained in the request was based upon user profile information located in a different device which created the cookie and then sent the cookie to the user's browser. The Applicants submit that the cookie contained in the user request, as stated above, can not be seen to relate to a determined attribute and a generated attribute certificate based in part on an automated scan of a first network device.

The Applicants submit that, for at least these reasons, Win can not be seen to disclose or suggest performing an automated scan of a second network device to determine at least one of a hardware or software capability of the second network device, as in claim 1.

Further, as cited Win discloses:

> "Access Server 106 stores a log-in page, Authentication Client Module and Access Menu Module. The Authentication Client Module authenticates a user by verifying the name and password with the Registry Server 108. If the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a "cookie" to the user's browser. [...] A cookie returned by the Authentication Client Module is required for access to resources protected by the system 2," (emphasis added), (col. 6, lines 41-54).

The Applicants note that Win, as cited above, appears to be applied in the Office Action in order

to support where the rejection alleges that Win suggests where claim 1 relates to storing the attribute certificate including the attribute on a device other than the second network device. The Applicants disagree with the rejection.

As stated above, it can be seen that as a result of an authentication using a correct user name and password the authentication client module merely reads the user's roles from the registry server 108 and then sends the information of the user's roles in a cookie to the user's browser. Therefore, in Win a cookie is determined and generated by a separate server using user role information found in the separate server. Then, according to Win the cookie is sent to the user's browser. The Applicants submit that Win can not be seen to disclose or suggest at least where claim 1 recites in part "storing the attribute certificate including the attribute **on a device other than the second network device**." This is seen to be the case for at least the reason that the cookie in Win is seen to be stored in the user's browser which is an equivalent of the second network device as in claim 1.

Further, in the Office Action the Examiner states:

> "Win does not explicitly teach determining at least one of a hardware or software capability of the second network and determining an attribute based, in part, on the determined capability," and
>
> "Wright teaches the feature of determining at least one of a hardware or software capability of the second network ([0013-0014], [00078]) and determining an attribute based, in part, on the determined capability ([0066-0067], [0078]-[0121])," and
>
> "It would have been obvious to one of ordinary skill in the Data Processing art at the time of the invention was made to modify the teachings of Wright into Win to include the feature of determining at least one of a hardware or software capability of the second network and determining an attribute based, in part, on the determined capability because it would have provided different levels of security protection for different location and/or security features are highly desirable for network device," (emphasis added).

The Applicants disagree with the Examiner. The Applicants contend that one of ordinary skill in

the art would not be motivated to combine Win and Wright for at least the reason such a combination would go against the teaching of Win which relates to providing a large scale system which adapts to millions of potential users.

Win discloses:

> "This need exists in the context of internal Web networks that are available to employees of an organization, called Intranets, as well as Web networks and resources that are available to external customers, suppliers and partners of the organization, called extranets. Extranet users may require information from a large number of diverse sources, for example, product catalogs, customer databases, or inventory systems. **There may be millions of potential users**, the number of which grows dramatically as an organization prospers. **Thus, there is a need for a large-scale system that can provide selective access to a large number of information sources for a large number of users**," (emphasis added), (col. 1, lines 45-55); and
>
> "There is a need for such a mechanism that is integrated with a flexible, adaptable, additive data model that **permits rapid and convenient addition of information describing users** and resources, and that **automatically propagates the effects of changes in the data model** throughout the system," (emphasis added), (col. 2, lines 34-38).

The Applicants submit that the method described in Wright is designed for corporate networks and enterprise systems where the devices of this system are seemingly well controlled. Implementing the system of Wright with Win, as proposed in the rejection, would at least require that all the client and server devices of Win be modified to include at least some of the modules of Wright. Further, the Applicants submit that these modifications would be most excessive, if even possible.

For example, the Applicants submit that to "modify the teachings of Wright into Win" in order to provide "different levels of security protection for different location[s] and/or security features," as indicated by the Examiner in the rejection, Win would be required to implement in each access server or mobile device the system 200 of Wright which is illustrated in Figure 2A. The system 200 of Wright "comprises an authorization module 232, a policy distribution module 234, a

policy management module 236," (par. [0047]). In addition, with regards to the client device, Wright illustrates the required modules in Figure 2B. In most applicable terms, the modules required (a partial list) in each of the large number of client devices in Win would include a location detection module 208 and a security features determination module 210, as illustrated in Figure 2B of Wright. Further, the Applicants submit that it is not clear if these particular modules will even function as intended without the other modules defined in Wright.

The Applicants submit that, for at least these reasons, a person of ordinary skill in the art who wishes to fill a need for a large-scale system that can provide selective access to a large number of information sources for a large number of users, as intended by Win, would not be motivated to combine Win and Wright. The Applicants submit that this is seen to be the case for at least the reason that implementing the modules of Wright in Win would clearly go against the "rapid and convenient addition of information describing users," and the "large-scale system that can provide selective access to a large number of information sources for a large number of users" as explicitly sought by Win, as stated above.

The Applicants contend that, for at least the reasons stated above, the proposed combination of Win and Wright would at least render Win unsatisfactory for its intended purpose and change the principal operation of Win.

MPEP 2143.01 V

THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE

If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984) (Claimed device was a blood filter assembly for use during medical procedures wherein both the inlet and outlet for the blood were located at the bottom end of the filter assembly, and wherein a gas vent was present at the top of the filter assembly. The prior art reference taught a liquid strainer for removing dirt and water from gasoline and other light oils wherein the inlet and outlet were at the top of the device, and wherein a pet-cock (stopcock) was located at the bottom of the device for periodically removing the collected dirt and water. The reference further taught that the separation is assisted by gravity. The Board concluded the claims were prima facie obvious, reasoning that it would

have been obvious to turn the reference device upside down. The court reversed, finding that if the prior art device was turned upside down it would be inoperable for its intended purpose because the gasoline to be filtered would be trapped at the top, the water and heavier oils sought to be separated would flow out of the outlet instead of the purified gasoline, and the screen would become clogged.).

"Although statements limiting the function or capability of a prior art device require fair consideration, simplicity of the prior art is rarely a characteristic that weighs against obviousness of a more complicated device with added function." In re Dance, 160 F.3d 1339, 1344, 48 USPQ2d 1635, 1638 (Fed. Cir. 1998) (Court held that claimed catheter for removing obstruction in blood vessels would have been obvious in view of a first reference which taught all of the claimed elements except for a "means for recovering fluid and debris" in combination with a second reference describing a catheter including that means. The court agreed that the first reference, which stressed simplicity of structure and taught emulsification of the debris, did not teach away from the addition of a channel for the recovery of the debris.).

MPEP 2143.01 VI

THE PROPOSED MODIFICATION CANNOT CHANGE THE PRINCIPLE OF OPERATION OF A REFERENCE

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation, whereas the claimed invention required resiliency. The court reversed the rejection holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

The Applicants contend that, for at least the reasons as stated above, the proposed combination of Win and Wright is seen to be improper.

The Applicants contend that, for at least the reasons stated above, the references cited can not be seen to disclose or suggest at least where claim 1 recites in part:

> "**performing an automated security scan of a second network device by a first network device** to determine at least one of a hardware or software capability of the second network device; **determining an attribute for the second network device based, in part, on the determined capability; generating an attribute certificate for the second network device based in part on the attribute; storing the attribute certificate including the attribute on a device other than the second network device**".

Thus, the Applicants submit that, for at least these reasons the rejection of claim 1 is seen to be improper and the rejection should be removed.

Reference item 2:

The Applicants submit that neither Win nor Wright, alone or combined, can be seen to disclose or suggest at least where claim 1 relates to receiving, at the first network device, an authentication request from the second network device for access to a resource over a network; **verifying the authentication request** from the second network device, **or else terminating communication with the second network device.**

As cited Win discloses:

> "The user enters the name and password into the login page using browser 100, which provides the name and password to Access Server 106. [...] **If the name and password cannot be authenticated** or the account is marked inactive, then as shown by state 512, **Access Server 106 returns an error message to browser 100**," (emphasis added), (col. 9, lines 51-60); and
>
> "For each login attempt, the Login Tracking Service logs the user's login activity. It saves the time of last successful and unsuccessful logins and **number of consecutive, unsuccessful login attempts**. The last successful and unsuccessful login times are displayed to the user after each successful login. Users can thus detect if someone else has attempted to use their account," (emphasis added), (col. 9, lines 60-67).

The Applicants submit that Win can not be seen to relate to terminating communication with a device as an alternative to verifying an authorization request. Rather, it can be seen that as a

result of an unsuccessful login attempt, as stated above, the access server of Win merely **returns an error message**. Further, the Applicants submit that modifying Win to terminate communication with a device in response to an unsuccessful authentication request (e.g., not verifying the authentication request) would not be obvious to one of ordinary skill in the art for at least the reason that, as stated above Win discloses motivation where Win discloses providing the number of consecutive unsuccessful logins to the user so that they can detect whether someone else has attempted to use their account.

Further, Wright can not be seen to overcome this shortfall of Win for at least the reason that Wright discloses:

> "the authorization module 232 authorizes **a communication exchange between the client mobile device and the policy distribution or policy management modules**. [...] Various authorization protocols and techniques may be used. One example is a simple **username and password verification** scheme," (emphasis added), (par. [0052]); and
>
> "In the illustrative context of FIG. 2A, the authorization module 232 receives 322 the status request with authorization information from a client mobile device, and **it determines 324 whether a communication exchange with this mobile device is authorized. If not, the status request is ignored 326 or an error message is sent 326**," (emphasis added), (par. [0128]).

The Applicants submit that it can be seen that for the case an authentication request not being verified, both Win and Wright are seen to ignore the authentication request and send an error message. The Applicants contend that, for at least these reasons, neither of the references cited can be seen to disclose or suggest at least where claim 1 relates to receiving, at the first network device, an authentication request from the second network device for access to a resource over a network, and **verifying the authentication request** from the second network device, **or else terminating communication with the second network device**. The Applicants submit that for at least this reason the references cited can not be seen to disclose or suggest claim 1 and the rejection should be removed.

Reference item 3:

First, the Applicants submit that, for at least the reasons as stated above, neither Win nor Wright can be seen to disclose or suggest an attribute certificate generated from a determined attribute which is based on an automated scan of a device by another device. The Applicants contend that for at least this reason the references cited can not be seen to disclose or suggest this identified item of claim 1.

However, the Applicants submit that assuming aurguendo that either operations relating to the cookie of Win or the security policy of Wright can somehow be seen to suggest determining and generating an attribute certificate as stated above for claim 1, though not agreed to for at least the reasons already stated, the Applicants contend that the references cited would still fail to disclose or suggest at least where claim 1 recites in part:

> "**responsive to a verified authentication request from the second network device** for access to a resource over a network, the first network device **requesting and receiving from the other device the stored attribute certificate for the second network device**; and **the first network device determining whether the received attribute certificate for the second network device is valid**, where if the attribute certificate is determined valid, authorizing access to the resource over the network, **or else terminating communication with the second network device**"

First, the Applicants submit that the cookie in Win is not seen to be requested in response to verifying an authentication by a device. Rather, as cited, Win discloses that:

> "**After a user is authenticated, the Authentication Client module 414 calls the Authorization service of Access Server 106. In response, the Authorization service requests profile information about the user from the Registry Server 108**, as shown by state 520. [...] The profile information may comprise the user's name, locale information, IP address, and information defining roles held by the user. **The Authorization service creates a "user cookie" 528 and "roles cookie" 530, which are used to convey profile information to browser 100.** The "user cookie" contains a subset of the user profile information. The "roles cookie" contains a list of the user's roles," (emphasis added), (col. 10, lines 43-

54).

Thus, it can be seen that, after the user is authenticated, the authentication client module of the access server in Win calls for the authorization service to create a cookie based upon the user's profile information. Then, as indicated above, this cookie is sent to the client browser 100. Thus, the Applicants submit that the cookie in Win is not being sent to an authenticating device which receives an authentication request from a client. Rather, the cookie is being sent to the client who has been authenticated. Therefore, Win can not be seen to disclose or suggest at least where claim 1 recites in part "**requesting and receiving from the other device the stored attribute certificate for the second network device**." The Applicants submit that, for at least this reason, claim 1 is distinguishable from Win.

Further, it is noted that, as cited Win discloses, that "A user is considered authenticated if the request contains a "user cookie" that can be decrypted, and the request's IP address matches that in the cookie" (col. 8, lines 28-31). However, as stated above, the Applicants submit that this operation of confirming that the IP address matches the cookie is performed by a runtime module on the protected server to which the user wishes access (see Fig. 2). The Applicants submit that for at least the reason that the protected server did not perform a verifying of the authentication request from the user and then, **responsive to the verifying**, receive the cookie for the user (alleged attribute certificate). Rather, as stated in Win the runtime module of the protected server must first contact an authentication verification service outside the protected server to check if a user making a request to the protected server **has already been authenticated**.

The Applicants submit that, for at least these reason, it can be seen that the decrypting of the "user cookie" and the determination of matching IP addresses is not performed "**responsive to a verified authentication request from the second network device** for access to a resource over a network," as in claim 1. Rather, Win is seen to simply verify authentication after receiving a user request which includes the cookie.

Moreover, with regards to the required matching IP address and decryption of the cookie Win

discloses that "If the conditions are not satisfied, then the user cannot be authenticated, and as shown in state 314, Runtime Module 206 returns a redirection to the Login URL," (col. 8, lines 31-33). Therefore, for the case that the IP address of the cookie is not matching Win discloses that the user is **redirected to a login URL**. The Applicants note that, here, Win can not be seen to relate to terminating communication with the user. The Applicants submit that here Win can not be seen to disclose or suggest at least where claim 1 recites in part "where if the attribute certificate is determined valid, authorizing access to the resource over the network, **or else terminating communication with the second network device.**"

Further, the Applicants submit that Wright can not be seen to overcome at least this shortfall of Win. Wright discloses:

> "The illustrated system 201 embodiment in accordance with the present invention further comprises a security feature module 210 for determining **whether one or more security features have an activity status of inactive or active in a communication session between the mobile device and another computer**," (emphasis added), (par. [0066]).

The Applicants submit that, here, Wright discloses that the **client mobile device** (see Fig. 2B) determines whether one or more security features is inactive or active. The Applicants can not find anything in all of Wright which can be seen to relate to a first network device, which has verified an authentication request, to determine whether an attribute certificate for a second network device is valid, and if not valid then terminating communication with the second network device.

The Applicants submit that, for at least this reason, neither Win nor Wright, alone or combined, can be seen to disclose or suggest at least where claim 1 recites in part:

> "**responsive to a verified authentication request from the second network device** for access to a resource over a network, the first network device **requesting and receiving from the other device the stored attribute certificate for the second network device**; and **the first network device determining whether the received attribute certificate for the second**

> **network device is valid**, where if the attribute certificate is determined valid, authorizing access to the resource over the network based, in part, on the attribute associated with the attribute certificate, **or else terminating communication with the second network device**"

The Applicant contends that, for at least the reasons stated, the references cited can not be seen to disclose or suggest claim 1 and the rejection of claim 1 should be removed.

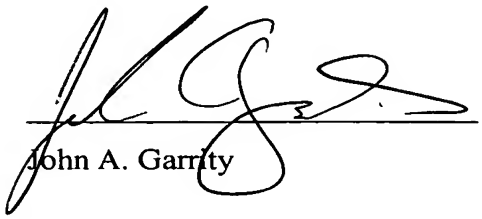
In addition, as the independent claims 9, 14, and 16 recite a feature similar to claim 1 as stated above, the references cited are not seen to disclose or suggest all claims 1, 9, 14, and 16. Therefore, the rejections of these claims should be removed.

Furthermore, for at least the reason that the claims 3-8; and 10 and 12-13; and 15; depend from claims 1, 9, and 14 respectively, the references cited are not seen to disclose or suggest these claims, and the rejections of all claims 1, 3-10, and 12-16 should be removed.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1, 3-10, and 12-16. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1, 3-10, and 12-16 and to allow all of the pending claims 1, 3-10, and 13-16 as presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' agent at the telephone number indicated below.

Respectfully submitted:



John A. Garrity

6/5/09

Date

S.N.: 10/823,378
Art Unit: 2453

Reg. No.: 60,470

Customer No.: 29683

HARRINGTON & SMITH, PC

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: jgarrity@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

6/5/2009
Date

Elaine F. Mian
Name of Person Making Deposit